UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

In the Matter of the Search of:	)	
	)	
Information Stored at Premises Controlled by Google, as further described in Attachment A	)	Case No. 20 M 297
	)	
	)	Magistrate Judge M. David Weisman

SEALED MEMORANDUM OPINION AND ORDER

Before the Court is the government's application for a geofence warrant. For the following reasons, the Court denies the warrant application.

Background

The government has submitted an application for a geofence warrant to Google, that is a warrant to obtain cellular phone data generated in a designated geographic area, during three forty-five minute periods of time on three different dates. The government seeks the warrant to further its investigation into the theft and resale of certain pharmaceuticals.

As to the first geofence request, the government has probable cause to believe that the suspect received the stolen pharmaceuticals from a commercial enterprise located within the designated geofence area during the designated forty-five minute interval in the early afternoon hours on the day of the first geofence request. The geofence, which has a 100-meter radius, is in a densely populated city, and the area contains restaurants, various commercial establishments, and at least one large residential complex, complete with a swimming pool, workout facilities, and other amenities associated with upscale urban living.[1]

The second and third geofence requests focus on the same commercial enterprise[2] where the government has probable cause to believe that the suspect shipped some of the stolen pharmaceuticals to a buyer, who purchased the pharmaceuticals from the suspect at the government's direction. Again, the government's requested geofence is a 100-meter radius area extending from the commercial establishment where the suspect shipped the pharmaceuticals and covers two separate dates for forty-five minute intervals in the early afternoon hours. This geofence includes medical offices and other single and multi-floor commercial establishments that are likely to have multiple patrons during the early afternoon hours.

---

[1] As evidence that Google applications are ubiquitously used, the Court relied on Google Maps and Google to gather information about the residential structures within the proposed geofence.

[2] For clarity's sake, the first geofence uses one business as its center point in defining the geofence. The second and third geofences use a different business as their center point, and that business is the same business for the second and third geofences.

The warrant application contemplates that the information will be obtained in three stages: (1) Google will be required to disclose to the government an anonymized list of devices that specifies information including the corresponding unique device ID, timestamp, coordinates, and data source, if available, of the devices that reported their location within the geofence during the forty-five minute periods; (2) the government will then review the list to prioritize the devices about which it wishes to obtain associated information; and (3) Google will then be required to disclose to the government the information identifying the Google account(s) for those devices about which the government further inquires. The warrant application includes no criteria or limitations as to which cellular telephones government agents can seek additional information. Further, the warrant application describes the items to be seized as follows:

> All information described above in Section I that constitutes evidence or instrumentalities of violations of the dispensing of a controlled substance by means of the internet without a valid prescription, in violation of 21 U.S.C. § 829(e)(1); the theft of medical products, in violation of 18 U.S.C. § 670; mail fraud, in violation of 18 U.S.C. § 1341; and wire fraud, in violation of 18 U.S.C. § 1343, that have been committed on or about [Date 1], [Date 2], and [Date 3], involving one or more unknown persons.

Discussion

The Fourth Amendment states:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. Const. amend. IV.

> [T]wo distinct constitutional protections [are] served by the warrant requirement. First, the magistrate's scrutiny is intended to eliminate altogether searches not based on probable cause. The premise here is that any intrusion in the way of search or seizure is an evil, so that no intrusion at all is justified without a careful prior determination of necessity. The second, distinct objective is that those searches deemed necessary should be as limited as possible. Here, the specific evil is the 'general warrant' abhorred by the colonists, and the problem is not that of intrusion per se, but of a general, exploratory rummaging in a person's belongings. The warrant accomplishes this second objective by requiring a 'particular description' of the things to be seized.

Coolidge v. New Hampshire, 403 U.S. 443, 467 (1971) (internal citations omitted).

Though "a search warrant [must] describe the objects of the search with reasonable specificity, it need not be elaborately detailed." *United States v. Somers*, 950 F.2d 1279, 1285 (7th

Cir. 1991). "The level of specificity must be such, however, that the officers executing the warrant are 'able to identify the things to be seized with reasonable certainty.'" *United States v. Sleet*, 54 F.3d 303, 307 n.1 (7th Cir. 1995) (quoting *United States v. Spears*, 965 F.2d 262, 277 (7th Cir. 1992)); *see also United States v. Vitek Supply Corp.*, 144 F.3d 476, 481 (7th Cir. 1998) ("[A] warrant must explicate the items to be seized only as precisely as the circumstances and the nature of the alleged crime permit.").

A search warrant contains two specificity requirements, which work in tandem. *See Archer v. Chisholm*, 870 F.3d 603, 614 (7th Cir. 2017) (a valid search warrant must "describe with particularity the things to be seized and the place to be searched"); *United States v. Hill*, 459 F.3d 966, 973 (9th Cir. 2006) ("[s]pecificity has two aspects: particularity and breadth"). First, the place to be searched must be described with particularity. *See, e.g., United States v. Nafzger*, 965 F.2d 213, 215-16 (7th Cir. 1992) (holding "Western District of Wisconsin" insufficiently particular to meet Fourth Amendment standards). Second, the items to be searched for must be particularly described. "To determine whether a specific warrant meets the particularity requirement, a court must inquire whether an executing officer reading the description in the warrant would reasonably know what items are to be seized." *United States v. Hall*, 142 F.3d 988, 996 (7th Cir. 1998). "In practice, courts have . . . demanded that the executing officers be able to identify the things to be seized with reasonable certainty and that the warrant description must be as particular as circumstances permit." *United States v. Jones*, 54 F.3d 1285, 1290 (7th Cir. 1995) (quoting *United States v. Brown*, 832 F.2d 991, 996 (7th Cir. 1987)); *see also Groh v. Ramirez*, 540 U.S. 551, 557 (2004) (a constitutionally valid search warrant must be based on probable cause, supported by a sworn affidavit, describe the place to be searched with particularity, and describe the items to be seized with particularity).

The level of particularity required as to what agents can seize is inversely related to the quality and breadth of probable cause established in the warrant application. "The Constitution requires that the warrant particularly describe the things to be sought and seized, but when there is probable cause to seize every business paper on the premises, a warrant saying seize every business paper particularly describes the things to be searched for and seized." *United States v. Bentley*, 825 F.2d 1104, 1110 (7th Cir. 1987) (quotations omitted); *see also United States v. Oloyede*, 982 F.2d 133, 140-141 (4th Cir. 1992) (collecting cases for the same proposition); *United States v. Griffin*, No. 11-CR-30, 2011 WL 3348030, at *13 (E.D. Wis. June 22, 2011) ("[h]ow detailed the warrant must be follows directly from the nature of the items there is probable cause to seize; detail is necessary only to the extent the judicial officer must limit the search and seizure to those items"); *United States v. Mason*, No. 92-CR-1069, 1993 WL 191806, at *2 (N.D. Ill. June 4, 1993) ("[W]here there is probable cause to seize all documents relating to a particular person, place or thing, the warrant can be broadly worded because it is unnecessary to distinguish between the things that may be taken from those that must be left undisturbed. In such cases, a generic description adequately defines the officers' authority [to search for particular items].").

Concerns that a search warrant is overbroad or lacking in particularity can be avoided by either properly incorporating an affidavit in a search warrant or, in limited circumstances, by having an officer share his knowledge that there is a particular place to be searched with the approving magistrate judge at the time the warrant is issued. *Nafzger*, 965 F.2d at 215; *see also United States v. Wenzel*, 854 F.3d 957, 961 (7th Cir. 2017) (search warrant for items related to

hidden-camera recordings satisfied constitutional requirements when several concrete categories of items were listed in supporting affidavit and probable cause existed); *Jones*, 54 F.3d at 1290-92 (7th Cir. 1995) (upholding a search warrant for "U.S. currency" without any more specifics because an unattached affidavit supplied some specific serial numbers the officers were seeking, which was known by the officer and the magistrate judge at the time the warrant was issued).

The Government's Proposed Warrant

The warrant presented in this matter suffers from two obvious constitutional infirmities. First, the scope of the search is overbroad, and second, the items to be seized are not particularly described. As to the scope of the warrant, the government is seeking all of the data of the cellular telephones that accessed Google applications or used Google's operating system in the three requested geofences. In its affidavit, the government asserts that approximately 97% of smartphones in the world use Google applications or Google's operating system.[3] Moreover, the area covered by each of the geofence applications is large, and the majority of the area sought encompasses structures and businesses that would necessarily have cell phone users who are not involved in these offenses. Each geofence encompasses 7.7630627 acres of land.[4, 5] Despite the geographic and practical reach of the geofences, the government's evidence of probable cause is solely focused on one user of a cellular telephone. As to the particularity of the items for which the government can search, the warrant application is completely devoid of any meaningful limitation. The application indicates that agents will be searching for "evidence or instrumentalities of" the listed offenses, but nothing more. *Massachusetts v. Sheppard*, 468 U.S. 981, 988 n.5 (1984) ("[t]he uniformly applied rule is that a search conducted pursuant to a warrant that fails to conform to the particularity requirement of the Fourth Amendment is unconstitutional").

Because of these apparent constitutional deficiencies, the Court requested that the government provide a legal memorandum justifying its warrant application. The government's response did not alleviate the Court's concerns.

---

[3] The percentage may not be this high. For example, Apple iPhones do not use Google's operating system to function, so an Apple iPhone would only be implicated by this search warrant if the user also used Google apps such as Gmail, Google Maps, Google Chrome and YouTube. And, even an Android phone user (who must use Google's operating system) could avoid coverage of this warrant if the user chose not to use Google location services. But, in establishing probable cause, the government asserts a likelihood "that at any given time, a mobile telephone, regardless of make, is interfacing in some manner with a Google application, service, and/or platform[.]" (Dkt. 3 at 11.) We assume this reasonable conclusion to be true, and thus reasonably conclude that likely hundreds of cellphones other than the suspect's cellphone would be included in the requested geofences.

[4] The area of a circle equals radius squared times pi. In this case, the area of the geofence is 31,416 square meters. One thousand square meters equal 0.247105 acres. And, of course, this quick calculation does not factor in that the areas in question contain multi-story buildings, which only adds to the actual "area" of the search.

[5] For purposes of comparison, Wrigley Field encompasses roughly eight acres, Solider Field encompasses seven acres, and Guaranteed Rate Field encompasses about twelve acres. *See* Dayn Perry, *The White Sox ballpark in Chicago that never was and could have changed history*, CBSSPORTS.COM (April 10, 2018), https://www.cbssports.com/mlb/news/the-white-sox-ballpark-in-chicago-that-never-was-and-could-have-changed-history/#:~:text=New%20Comiskey%2FU.S.%20Cellular%20Field,meantime%2C%20occupies%20about%2012%20acres.; *see also Soldier Field*, WIKIPEDIA, https://en.wikipedia.org/wiki/Soldier_Field (last visited July 8, 2020).

The Government's Request for a Search Warrant and Controlling Precedent

The government cites no controlling authority, and this Court has found none, that addresses the legal standards to be applied to a geofence warrant. Thus, as reflected *supra*, we apply general principles of Fourth Amendment law that courts have developed in assessing the constitutional validity of search warrants.

Here, the search warrant is directed at Google, and effectively seeks Google's records regarding its customers. In its memorandum, the government notes that "[t]he Supreme Court 'has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed [by the third-party] to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.'" (Dkt. 3, n.1) (quoting *United States v. Miller*, 425 U.S. 435, 443 (1976)). In *Miller*, the Supreme Court held that the government properly obtained the defendant's bank records through a subpoena, as opposed to securing a search warrant, because the subject of the investigation had voluntarily allowed the bank to gather the information reflected in the subpoenaed documents. *Id*. at 443-46.

The government then distinguishes its warrant application from the Supreme Court's more recent holding in *United States v. Carpenter*, 138 S. Ct. 2206 (2018) that cell-site records of seven days or more are not subject to the "third-party doctrine" memorialized in *Miller*. The purpose of this explication is unclear. If the government believes that the information it seeks from Google can be obtained by a grand jury subpoena (or some other process), then it should proceed in that manner. But the government seeks a search warrant and offers no justification for jettisoning traditional standards of Fourth Amendment jurisprudence in the context of a geofence warrant. Therefore, this Court will proceed by applying developed constitutional standards to a newly-developed investigative tool.

The Government's Response

We start with our only point of agreement with the government's response. There is probable cause to believe that among all the other data this warrant application seeks from Google, there is a likelihood that the suspect's phone data would be included. Probable cause, however, is only part of the recipe for a constitutionally valid search warrant. *See Groh*, 540 U.S at 557.

The government offers two factual arguments to justify its request for permission to identify all cellular phones located in the geofences. First, the government asserts that "[t]he identification of devices that were located at or near the [targeted stores] immediately before, during, and after the receipt and shipping of the stolen prescription medication is evidence of the Subject Offenses, namely, evidence pertaining to the identity of the Unknown Subject and *any possible co-conspirators.*" (Dkt. 3 at 11) (emphasis added). There is no evidence in the application's supporting affidavit that the suspect is conspiring with anyone to commit these offenses, and the evidence developed by the government to date does not reasonably suggest there are co-conspirators. Simply put, there is not probable cause to believe the government will find evidence linking co-conspirators to the described offenses.

Next, the government argues that "other individuals with cellular devices who were within a 100-meter radius of the [targeted stores] during the time periods covered by the proposed Warrant would be potential witnesses to the crime" and "[i]nformation identifying one or more of such witnesses is evidence." (Dkt. 3, n.3.) This argument strains credibility.[6] The obvious witnesses to these offenses are the employees at the targeted businesses who assisted the suspect in the transactions involving the stolen pharmaceuticals. Those individuals can be, and likely have been, identified by the government through other means. Moreover, the notion that individuals in the area would be witnesses to the offense (thus supporting another basis for probable cause to justify the geofence) is not mentioned in the government's affidavit. The affidavit premises probable cause on the identification of the subject of the investigation, not on identification of potential witnesses.

The government next posits an unsubstantiated legal argument to address the apparent overbreadth of the scope of the warrant. The government asserts "the Search Warrant was narrowly tailored based on location, date, and time" (*id.* at 12) but offers no case law or governing Fourth Amendment principles to justify this assertion. While we agree that the date and time are sufficiently prescribed, the location clearly is not. As noted *supra*, the geographic scope of this request in a congested urban area encompassing individuals' residences,[7] businesses, and healthcare providers is not "narrowly tailored" when the vast majority of cellular telephones likely to be identified in this geofence will have nothing whatsoever to do with the offenses under investigation.

Finally, as to the particularity required by the Fourth Amendment, the government's approach fares no better. The government argues:

> The Search Warrant included a multi-step execution process that would require Google to identify the user of a device only if, *based on the location information provided by Google*, it appears that the device is relevant to the investigation. Rather than violating the Fourth Amendment, this multi-step process would allow

---

[6] The government's position that it should be able to identify all of the people within these 7.7 acres of land to see if any might recall the suspect and be able to identify the suspect is disconcerting at best. These potential witnesses would truly be remarkable. They would likely need to possess extremely keen eyesight and perhaps x-ray vision to see through the many walls (both interior and exterior) of the structures they inhabited during the time periods at issue. Moreover, their memories would have to be of the kind that allows the most mundane events to be seared in their memories. Recall, the circumstances of these geofence applications are routine business events. The suspect received a mailed package or mailed packages. This is not a protracted bank robbery, a remarkable act of violence, or an unusual event of any sort that might conceivably draw bystanders' attention.

[7] The government's inclusion of a large apartment complex in one of its geofences raises additional concerns. The government's position that it may obtain location information as to an individual who may be in the privacy of their own residence without any showing of probable cause related to that individual or her residence may run afoul of Fourth Amendment cases that require a warrant to obtain such information. *See Kyllo v. United States*, 533 U.S. 27, 34 (2001) ("[w]e think that obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical intrusion into a constitutionally protected area, constitutes a search—at least where (as here) the technology in question is not in general public use.") (quotations omitted). *But see United States v. Caira*, 833 F.3d 803, 809 (7th Cir. 2016) (holding that obtaining the IP address used by the defendant from his house was proper under the third-party doctrine). Because we find the warrant application deficient for other reasons, we do not need to resolve whether *Kyllo* applies to geofencing technology.

> investigators to further protect people's privacy in the event that investigators determined a particular device is likely not associated with the Unknown Subject, any possible co-conspirator, or any witness to the Unknown Subject's receipt or shipping of the stolen prescription medication.

(Dkt. 3 at 13) (emphasis added).

This argument fails on multiple levels. First, it is factually untrue. There is no objective measure that limits the agents' discretion in obtaining information as to each cellular telephone in the geofence. For example, the warrant does not limit agents to only seeking identifying information as to the "five phones located closest to the center point of the geofence," or some similar objective measure of particularity. As already noted, the geographic range coupled with the urban nature of the encompassed area ensures an overbroad scope of the identified cellular phones. If the warrant did contain objective limits as to which cellular telephones agents could seek additional information, or the nature of the probable cause established in the warrant application suggested a very limited number of cellular telephones would be identified, the Court's concern with overbreadth and particularity might be satisfied.[8] However, this multi-step process simply fails to curtail or define the agents' discretion in any meaningful way.

Second, the government cites inapposite legal authority with respect to the particularity requirement. The government relies on *United States v. McLamb*, 880 F.3d 685 (4th Cir. 2018) and a series of cases that address the legality of computer searches generated by a cutting-edge investigative tool employed by the FBI to identify computers that reached a server on the dark web known as Playpen, where users could upload or download child pornography. "In order to access [the Playpen website], a user [had to] download [a separate encrypted online network] and enter the site's domain name, a 16–character URL consisting of random letters and numbers. Playpen was not discoverable on the open web, nor could a search engine like Google route users to it." 880 F.3d at 688. The warrant obtained in those cases allowed agents to obtain identifying information "of any user or administrator who log[ged] into [Playpen] by entering a username and password." *United States v. Matish*, 193 F. Supp. 3d 585, 594–95 (E.D. Va. 2016). Courts that considered this issue unanimously found that the warrant sufficiently described computers that agents could "search."[9] *See id.* at 609 (because the warrant was based on probable cause that any computer that reached Playpen was involved in possessing or trading child pornography, agents' discretion as to which computers were actually searched did not violate constitutional standards).

The analysis employed in these cases is completely consistent with Fourth Amendment standards. The executing officers were able to identify the things to be seized with reasonable certainty, and the warrant's description was as particular as the circumstances permitted. *Jones*, 54 F.3d at 1290 (7th Cir. 1995). Agents could only seize identifying information relating to computers that tunneled through the dark web to find the Playpen website and, based on the

---

[8] For example, the government, in an unrelated case, sought a geofence warrant for an almost empty commercial parking lot where only one vehicle was located, according to the supporting affidavit. Two occupants of the vehicle were observed engaging in a criminal act, and then the vehicle left the parking lot. The nature of the probable cause justifying the warrant avoided any overbreadth issue and addressed the particularity requirement necessary for a valid warrant.

[9] The search consisted of acquiring identifying information as to the computer's location.

investigation's results at the time the warrant was obtained, the agents could not identify the offending computers with any greater particularity. The reasonableness of a warrant's particularity is judged based on what agents know and share with the magistrate judge at the time the warrant is obtained. *Maryland v. Garrison*, 480 U.S. 79, 85-86 (1987); *see also Jacobs v. City of Chi.*, 215 F.3d 758, 768 (7th Cir. 2000) ("[W]e conclude that although the warrant turned out to be overbroad because it did not describe with particularity the place to be searched and encompassed a separate dwelling unit, the plaintiffs' apartment, for which there was no probable cause to authorize a search, it was valid at the time it was issued based on the information the officers presented to the magistrate.").

The government argues that the line of reasoning employed in the Playpen cases "similarly applies to the multi-step execution process in the Search Warrant at issue here." (Dkt. 3 at 14.) In fact, the Playpen cases do not support the government's position in the least. In the Playpen investigation, for *every* computer that reached the Playpen cite, there was probable cause to believe the computer possessed evidence related to child pornography. The investigating agents could only seek identifying information for those computers that entered a website designed to promote the exchange of child pornography. The agents' discretion was limited by an objective standard – whether the computer logged into the Playpen website – which established probable cause that the computer was involved in criminal conduct. That analysis is the complete antithesis of the legal underpinning of the government's application in the instant case. The government has established probable cause that *one* user of a cellular telephone in the geofence area has committed a criminal offense. The warrant seeks to gather evidence on potentially *all* users of phones in the geofence, completely at the agents' discretion.

Without conceding its error, the government offers a modification to the search warrant that spells out in greater detail the type of information that agents could seek from Google. These additions do nothing to address the other level of particularity – as to which cellular phones agents may seek information. That determination remains solely in the agents' discretion, which the Fourth Amendment will not tolerate.

Conclusion

The government's warrant application suffers from overbreadth, lack of particularity, and provides no compelling reason to abandon Fourth Amendment principles in this case. *See, e.g.*, *Carpenter*, 138 S. Ct. at 2223 (allowing that "if law enforcement is confronted with an urgent situation, such fact-specific threats will likely justify the warrantless collection of" cell site location information even though obtaining such information generally requires a search warrant").[10] Most importantly, the government could easily have sought a constitutionally valid search warrant if it chose. For example, if the government had constrained the geographic size of the geofence and limited the cellular telephone numbers for which agents could seek additional information to those numbers that appear in all three defined geofences, the government would

[10] This Court's citation to *Carpenter* is not intended to suggest that *Carpenter* pre-ordains the outcome here. *Carpenter* involved a much longer period of time and greater data as to a particular subject's movements. This opinion is premised on much longer established Fourth Amendment principles that a search warrant must establish probable cause to justify the scope of the search requested, and the type of evidence to be seized must be particularly described, not left to the agents' complete discretion.

have solved the issues of overbreadth and lack of particularity. But, instead, the government chose to defend its position in ways that are not supported by the law and the facts and do not satisfy constitutional standards.

The government's use of geofences as an investigative tool is increasing exponentially. *See* Denise Lavoie, *Geofence Warrants to Be Tested in Virginia Bank Robbery Case*, ASSOCIATED PRESS (July 3, 2020), https://apnews.com/ae0dbee812feefe4f54d3539885f9f54 (Google stated that geofence warrant requests have "jumped 1,500% from 2017 to 2018, and another 500% [in 2019]."). The government's undisciplined and overuse of this investigative technique in run-of-the-mill cases that present no urgency or imminent danger poses concerns to our collective sense of privacy and trust in law enforcement officials.

As stated by the Supreme Court:

> It may be that it is the obnoxious thing in its mildest and least repulsive form; but illegitimate and unconstitutional practices get their first footing in that way, namely, by silent approaches and slight deviations from legal modes of procedure. This can only be obviated by adhering to the rule that constitutional provisions for the security of person and property should be liberally construed. A close and literal construction deprives them of half their efficacy, and leads to gradual depreciation of the right, as if it consisted more in sound than in substance. It is the duty of courts to be watchful for the constitutional rights of the citizen, and against any stealthy encroachments thereon.

Coolidge, 403 U.S. at 454 (quotation omitted). In short, because the warrant is overbroad both as to the scope of the search and the particularity of the items to be seized, and thus fails to comport with well-established Fourth Amendment jurisprudence, the Court denies the government's request for a warrant.

SO ORDERED.

ENTERED:

Dated: 7/8/2020

M. David Weisman

M. David Weisman
United States Magistrate Judge